# Incident Response Report

**Incident ID:** ZachM-20251205

**Date of Report:** 12.07.2025

**Report Prepared By:** Zach Maestas

### 1.0 Executive Summary

This incident response report documents defensive monitoring of three exposed services intended for red team exploitation: nginx decoy, PostgreSQL decoy, and SSH on metasploitable. The objective of said exercise was to detect exploitation attempts, capture authenticated access, and document attacker behaviors.

However, no successful nor unsuccessful attack traffic was recorded from the assigned red team partner. Instead, only routine instructional port verification scans (for the simulation) were observed. No shell access, brute force, database interaction, or credential misuse occurred according to the logs available.

Although no compromise took place, full forensic validation was performed across system logs, network capture points, and service-specific records to confirm the absence of a penetration test.

### 2.0 Detection and Analysis

**What Should Have Happened**

Based on the design of the lab, the expected actions were:

* Enumeration
* Exploitation of metasploitable
* Login to vulnerable ssh service on metasploitable

**What Actually Happened**

Only the automated CS 456 scans occurred:

* Port visibility checks
* No exploitation payloads
* No login attempts
* No brute force passwords
* No SQL auth failures

Logs reviewed

* Nginx access.log & error.log
* PostgreSQL protocol logs
* Metasploitable SSH auth logs
* System syslog
* Firewall logs

Expected but absent

* Root login from unknown
* Failed password for invalid user
* Metasploit handler IP callbacks
* PostgreSQL auth rejects

No attacker enumeration tooling (nmap -sV, sqlmap, hydra, msfconsole) appeared in logs.

### 3.0 Timeline of Expected Attack vs Actual

Note: *No deviation from baseline system states occurred.*

|  |  |  |
| --- | --- | --- |
| **Phase** | **Expected Red Team Action** | **Actual Observed Result** |
| Recon | |  | | --- | |  |  |  | | --- | | Perform nmap -sV against Metasploitable2 to  enumerate open services (FTP, SSH, DB, RPC) | | Light instructor port poll only |
| Exploit | Attempt exploitation against Metasploitable2 SSH via msfconsole (not vsftpd/unrealircd because those services were not present) | None |
| Shell Access | Attain remote session | None |
| Interaction | Minimal command execution solely to prove access | None |
| Post-Access | None required (no pivoting, no data theft, no persistence per assignment scope) | None |

### 4.0 Scope and Impact Assessment

Because no real attack took place:

* No confidentiality risk
* No integrity change
* No availability disruption

**Environment remained stable and untouched during the simulation.**

Containers, configs, and network segmentation prevented external tampering aside from the intentionally vulnerable service.

Impact Score: **None**

### 5.0 Containment, Eradication, and Recovery

No remediation was necessary because:

* No malware dropped
* No user accounts effected
* No metasploitable successful connections
* No evidence of tampering

**What was still done**

* Verified log retention
* Confirmed no log tampering
* Confirmed no privileged session openings

### 6.0 Recommendations and Lessons Learned

Despite exploitation never occurring, several takeaways are clear:

1. Logging Coverage Matters

* Instructor scans were still visible, demonstrating functionality

1. Missing Attack Traffic is Still Evidence

* Blue team must prove absence through verification

1. Decoy Services Should Remain Hardened

* Maintain segmentation, rotate ports, and log at balanced verbosity

1. Future Improvement

* Coordinate red/blue scheduling to ensure traffic exists when IR testing is required
* Enable alerting triggers when any authentication attempts hit decoys, not just successful shells.

**Primary Lesson Learned**

An IR report is valid even without compromise, as even if you suspect something MAY have happened, it is still crucial to investigate. Providing documentation proves why no incident was present, as it is revealed which logs were searched, what was absent, and why it was significant.